

APPLICATION FOR UNITED STATES LETTERS PATENT

FOR

AUTHENTICATION OF HTTP APPLICATIONS

Attorney docket: FSP0038

Client reference: AWS 856.US

Inventors: Bryan Sullivan

Prepared by: Charles A. Mirho

Patent Attorney

Reg. No. 41,199

Express Mail label number: EO902632469US

AUTHENTICATION OF HTTP APPLICATIONS

Technical Field

5 **[0001]** The present disclosure relates to software application authentication.

Background

10 **[0002]** Software and content piracy are significant problems. Each year, artists and software developers lose large sums of money to pirates who duplicate and/or distribute software and content without reimbursement to the owners. The advent of large-scale computing networks, such as the Internet, has exacerbated the problem, because content and software may be duplicated and distributed by pirates quickly and easily over large geographic areas.

15 **[0003]** Increasingly, content and software are being made available via wireless telephones. Wireless telephones are devices capable of transmitting and receiving voice and/or data (non-voice) information to and from a network without the use of wires, cables, or other tangible transmission media. So-called cellular telephones are a common
20 example of wireless phones.

25 **[0004]** Wireless telephones and the networks by which they communicate operate according to various technologies, including analog mobile phone service (AMPS), circuit switching, packet switching, wireless local area network (WLAN) protocols such as IEEE 802.11 compliant networks, wireless wide-area networks (WWAN), short-range RF systems such as Bluetooth, code division multiple access (CDMA), time division multiple access (TDMA), frequency-division multiplexing (FDM), spread-spectrum, global system for mobile communications (GSM), high-speed circuit-switched data (HCSD), general packet radio system (GPRS),
30 enhanced data GSM environment (EDGE), and universal mobile telecommunications service (UMTS). Of course, these are only examples, and other technologies may be employed in wireless communication as well.

[0005] Herein, the term 'wireless device' is meant to include wireless telephones (including cellular, mobile, and satellite telephones), and also to include a variety of other wireless devices, including wireless web-access telephones, automobile, laptop, and desktop computers that communicate wirelessly, and wireless personal digital assistants (PDAs). In general, the term 'wireless device' refers to any device with wireless communication capabilities. A wireless device may be a 'client device', which is any device that provides requests for services from a network. A 'server device' is a device of the network that receives and responds to client device requests. Of course, depending upon the circumstances, a client device may act as a server device, and vice versa.

[0006] Many companies produce wireless telephones and other wireless devices. Among the more well-known producers are Nokia®, Ericsson®, Motorola®, Panasonic®, Palm® Computer, and Handspring®. A variety of producers also provide wireless devices comprising versions of the Microsoft® Windows® operating software.

[0007] One method of content and software duplication involves "downloading", whereby a client device (such as a personal computer, music player, wireless telephone, and so on) communicates with a server device to obtain a copy of content and/or software available via the server device. Various protocols are available for downloading, including Hypertext Transfer Protocol (HTTP) and File Transfer Protocol (FTP).

[0008] Client logic is software of the client device that makes requests to the server for content/software. To prevent unauthorized behavior and/or piracy, the server may authenticate the client logic before fulfilling the requests. Where the client and server communicate via HTTP, the server may refer to the "User Agent" HTTP header for an identification of the client logic. For example, the HTTP header may identify the client logic as "WAP Browser for Nokia Phones version 1.5". The server may provide the requested content/software only to authorized client logic. Communication service providers (such as

AT&T Wireless Services and other entities that provide wireless communications to subscribers) may enter into arrangements with content and software providers to provide content and/or software for subscribers of the service providers. Thus, content and software (such as ring tones and games for a wireless telephone) may be provided by the server to a "WAP Browser for Phones" but not to another browser application that is not authorized to receive this content and software.

[0009] A problem with this approach is that authorized client logic may be "spoofed" by unauthorized client logic. For example, HTTP client logic may set the User-Agent header to identify itself to an HTTP server as an authorized client logic for content and software, when in fact the application is not so authorized.

Summary

[0010] The following summary is intended to highlight and introduce some aspects of the disclosed embodiments, but not to limit the scope of the invention. Thereafter, a detailed description of illustrated embodiments is presented, which will permit one skilled in the relevant art to make and use aspects of the invention. One skilled in the relevant art can obtain a full appreciation of aspects of the invention from the subsequent detailed description, read together with the figures, and from the claims (which follow the detailed description).

[0011] An apparatus acting as an HTTP proxy server, such as a Wireless Application Protocol (WAP) proxy/gateway, compares information of a request by client logic with a known pattern of information for an HTTP client logic, and when the information of the request matches the known pattern, causes content and/or software to be communicated to the client in response to the request. The apparatus may apply information provisioned to a client device comprising the HTTP client (such as a wireless phone or other wireless device) to interpret at least a portion of the information of the request. The interpreted information of the request may be compared

to information of the request identifying the client logic. the HTTP proxy may also validate or invalidate the request according to the result of the comparison.

5

Brief Description of the Drawings

[0012] The headings provided herein are for convenience only and do not necessarily affect the scope or meaning of the claimed invention.

10

[0013] In the drawings, the same reference numbers and acronyms identify elements or acts with the same or similar functionality for ease of understanding and convenience. To easily identify the discussion of any particular element or act, the most significant digit or digits in a reference number refer to the figure number in which that element is first introduced.

15

[0014] Figure 1 is a block diagram of an embodiment of an HTTP communication arrangement.

[0015] Figure 2 is a block diagram of an embodiment of a client device.

[0016] Figure 3 is a block diagram of an embodiment of an HTTP proxy.

20

[0017] Figure 4 is a block diagram of an embodiment of a wireless communication network.

[0018] Figure 5 is a block diagram of an embodiment of a coupling of a wireless network to an HTTP network.

[0019] Figure 6 is an action diagram of an embodiment of a method of authenticating an HTTP application.

25

[0020] Figure 7 is a flow chart of an embodiment of authenticating an HTTP application.

[0021] Figure 8 is a flow chart of an embodiment of a method of authenticating an application according to the total content of a protocol request.

30

Detailed Description

[0022] The invention will now be described with respect to various embodiments. The following description provides specific details for a thorough understanding of, and enabling description for, these

embodiments of the invention. However, one skilled in the art will understand that the invention may be practiced without these details. In other instances, well known structures and functions have not been shown or described in detail to avoid unnecessarily obscuring the description of the embodiments of the invention. References to “one embodiment” or “an embodiment” do not necessarily refer to the same embodiment, although they may.

[0023] Unless the context clearly requires otherwise, throughout the description and the claims, the words “comprise,” “comprising,” and the like are to be construed in an inclusive sense as opposed to an exclusive or exhaustive sense; that is to say, in the sense of “including, but not limited to.” Words using the singular or plural number also include the plural or singular number respectively. Additionally, the words “herein,” “above,” “below” and words of similar import, when used in this application, shall refer to this application as a whole and not to any particular portions of this application. When the claims use the word “or” in reference to a list of two or more items, that word covers all of the following interpretations of the word: any of the items in the list, all of the items in the list and any combination of the items in the list.

[0024] Herein, “logic” refers to any information having the form of instruction signals and/or data that may be applied to affect the operation of a processing device (processor). Examples of processors are computer CPUs (central processing units), microprocessors, digital signal processors, controllers and microcontrollers, and so on. Logic may be formed from signals stored in a device memory. Software is one example of such logic. Examples of device memories that may comprise logic include RAM (random access memory), flash memories, ROMS (read-only memories), EPROMS (erasable programmable read-only memories), and EEPROMS. Logic may also be comprised by digital and/or analog hardware circuits, for example, hardware circuits comprising logical AND, OR, XOR, NAND, NOR, and other logical operations. Herein, software is distinguished from hardware in that software does not comprise hardware elements,

whereas logic may be formed from combinations of software and hardware.

[0025] Figure 1 is a block diagram of an embodiment of an HTTP communication arrangement. A client device 102 comprises HTTP client logic 104, e.g. logic to provide HTTP communications with a server. The client device 102 communicates (wirelessly or via wires, cables, or other means) with an HTTP proxy 106. The HTTP proxy 106 represents the HTTP client 102 in HTTP communications with the network 108 (providing anonymity, security, and other benefits). The network 108 provides for communications between the HTTP proxy 106 and an HTTP server 110. The HTTP server 110 provides the HTTP client 104 with access to content and/or software via HTTP communications.

[0026] Figure 2 is a block diagram of an embodiment of a client device. The client device 102 comprises the HTTP client 104, provision information 210, operational logic 205, a processor 204, and a Subscriber Identity Module (SIM) 202. The SIM 202 identifies a subscriber of the network 108 by which the client device 102 communicates. A "subscriber" represents one or more persons or entities (corporations, partnerships, agents, operators, etc.) with access privileges to the network 108. A subscriber may be or represent a single user, or may represent one or more users. "User" refers to any person (or, conceivably, autonomous or semi-autonomous logic) with access privileges to the network 108. Typically the user is the operator of the client device 102, although a user could also be the operator of a device or devices that provide services via the network.

[0027] Some client devices 102 may not employ a SIM 202. In such devices a subscriber is typically associated with the client device 102 via logic 205 of the client device.

[0028] The logic 205 is applied to the processor to operate the client device 102. The HTTP client logic 104 is applied to the processor to provide HTTP communication with the network 108.

[0029] The provision information 210 is information communicated from the network 108 to the client device 102 and stored therein. For example, the provision information 210 may include an International Mobile Station Identifier (IMSI) for the device.

5 **[0030]** In some embodiments, the SIM 202 comprises a processor 214 and logic 212. The logic 212 of the SIM 202 may be applied to the processor 214 to operate the SIM 202 in cooperation with the operation of the client device 102. The SIM 202 may also comprise provision information 210. When the provision information 210 is
10 comprised by the SIM 202, the provision information 210 may be portable among different client devices 102 (by decoupling the SIM 202 from one device and coupling it with another). When no SIM is present, the provision information 210 is comprised by the client device 102.

15 **[0031]** Figure 3 is a block diagram of an embodiment of an HTTP proxy 106. The proxy 106 comprises a processor 306 and HTTP proxy logic 304 that, when applied to the processor 306, provides HTTP proxy services, may also perform authentication of the HTTP client 104 as described herein. The proxy 106 comprises at least one port 308 by
20 which HTTP communications may take place.

[0032] Figure 4 is a block diagram of an embodiment of a GSM network. Other types of communications networks, such as GPRS networks and networks of mixed technology, may also be employed. In the GSM network, a client device 102 communicates with a base
25 station subsystem (BSS) 445 comprising base station controllers (BSC) 420 coupled to one or more base transceiver stations (BTS) 425. In turn, each BTS 425 is coupled to one or antennae 430.

[0033] The BTS 425 includes transmitting and receiving equipment to create a radio interface between the wireless network and terminal
30 devices. Although the antennae 430 are shown as separate elements for clarity, it is common in the industry to collectively refer to the antennae 430, transmitter, and receiver, as the BTS.

[0034] The BSC 420 may perform management of the radio interface by allocating channels, managing handover from one BTS to another,

paging the wireless device, and transmitting connection-related signaling data.

5 **[0035]** The networking and switching subsystem (NSS) 435 of a wireless network comprises a Mobile Switching Center (MSC) 440, a Home Location Registry (HLR) 445, and a Visitor Location Registry (VLR) 450. Switching and network management functions are carried out by the NSS 435. The NSS 435 may also act as a gateway between the wireless network and other networks such as the Public Switched Telephone Network (PSTN), Integrated Services Digital
10 Network (ISDN), the Internet, corporate intranets, other wireless networks, and the Public Data Network (PDN).

15 **[0036]** The MSC 440 is a switching mechanism that routes communications and manages the network. In GPRS networks, GPRS support nodes (GSNs) such as Switching GSNs (SGSNs) and Gateway GSNs (GGSNs) may provide switching operations similar to those provided by the MSC 440. There can be many switches 440 in a communication network, each responsible for the signaling required to set up, maintain, and terminate connections to wireless devices within the geographical area served by the switch 440. Each MSC
20 (switch) 440 may manage several BSC 420. The MSC 440 is coupled to a Home Location Registry (HLR) 445 and a Visitor Location Registry (VLR) 450. The HLR 445 is also coupled to the VLR 450. The HLR 445 and VLR 450 may comprise certain dynamic or temporary subscriber data such as current Location Area (LA) of
25 the subscriber's mobile station and Mobile Station Roaming Number (MSRN). Subscriber-related data is recorded in the HLR 445 from which billing and administrative information is extracted when needed by the cellular service provider. Some wireless networks have only one HLR 445 that serves all subscribers; others have multiple HLRs.

30 **[0037]** The MSC 440 uses the VLR 450 to manage the wireless devices that are currently roaming in the area controlled by the MSC 440. The VLR 450 stores information such as the International Mobile Subscriber Identity (IMSI), authentication data, and telephone number of the roaming wireless devices. The VLR 450 may obtain and

comprise subscriber information, such as information about the services to which a roaming wireless device is entitled, from the HLR that serves the wireless device. The VLR 450 controls a pool of MSRN and allocates an MSRN and TMSI to the roaming wireless device. The VLR 450 sends the MSRN and Temporary Mobile Subscriber Identity (TMSI) information to the HLR 445 where they are stored with the subscriber's dynamic records for later use in call routing.

5
[0038] The operation subsystem (OSS) 455 may include an Equipment Identity Register (EIR) 460, an Authentication Center (AuC) 465, and an Operating and Maintenance Center (OMC) 470. The OSS 455 may provide subscription management, network operation, network maintenance, and mobile equipment management.

10
[0039] The AuC 465 stores data related to network security and authentication of wireless devices and subscribers. A purpose of the AuC 465 is to prevent fraud by verifying the identity of subscribers and/or devices that try to access the network. Thus the AuC 465 may comprise authentication algorithms and encryption codes necessary to protect a subscriber's access rights and identity and to prevent eavesdropping.

15
20
[0040] The EIR 460 is a database which stores International Mobile Equipment Identity (IMEI) numbers. Wireless devices are uniquely identified by an IMEI or equivalent number such as an Electronic Serial Number (ESN). An EIR 460 generally indicates the status of a particular wireless device by flagging the IMEI of a device identified stolen, suspended, or malfunctioning.

25
[0041] The OMC 470 monitors and controls other network elements to enhance system performance and quality. The OMC 470 also administers billing, subscriber service data, and generation of statistical data on the state and capacity of the network.

30
[0042] Figure 5 is a block diagram of an embodiment of a coupling of a network to an HTTP network. An HTTP network 504 is a network by which HTTP communication may take place. The network 108 is coupled to an HTTP proxy 502, by which the network 108 may

communicate with the HTTP network 504. The HTTP proxy 502 provides an interface between wireless network protocols and services, and Internet protocols and services. For example, the HTTP proxy 502 could provide an interface whereby communications from the HTTP server 110 involving Internet Protocol (IP), HTTP, and/or FTP, to name just a few, are communicated to the network 108 via Signaling System 7 (SS7) or other network communication methods. Communications from the network 108 involving SS7 or other wireless network protocols may likewise be converted by the HTTP proxy 502 to protocols supported by the HTTP network 504.

[0043] Figure 6 is an action diagram of an embodiment of a method of authenticating client logic. At 604 a network, such as a wireless network, communicates provision information to a client, and the client stores the provision information at 606. At 608 the client communicates a request to the server (e.g. an HTTP proxy server, or the HTTP server itself). The request comprises particular headers, in a particular sequence, comprising particular values. The client may include at least some of the provision information in the request. At 610 the server authenticates the client logic according to the information provided in the request. For example, the particular headers, sequence of the particular headers, and content of the particular headers provided in the request may strongly identify particular client logic. At 612 content (and/or software) requested by the client is provided by the server to the client, provided that the client is authenticated as a client that is authorized to receive the content and/or software.

[0044] Figure 7 is a flow chart of an embodiment of a method of authenticating client logic. At 702 the request information is provided to a server. At 704 a check is made to determine whether header types and/or header order and/or header content of the request matches known header patterns of a client that is authorized to receive the requested content (and/or software). If there is a match with an authorized client, the request is validated at 705, and in response to the valid request, the content is provided at 706. A

Otherwise the request is invalidated at 707, the content is not provided, and the method concludes at 708. A validated request is a request that has a form and content such that the server acts to fulfill the request. For example, a validated request may contain a key or other authentication information to indicate that the request comes from an authorized client and should be fulfilled.

[0045] By way of example, HTTP client logic conforming to Wireless Application Protocol Version 2.0 (WAP2) may communicate an HTTP request as a series of text strings separated by carriage return and line feed characters (e.g. lines). The first line may be the HTTP method (e.g. GET, HEAD, POST, etc.) containing the Universal Resource Identifier (URI) and the protocol version. The method line may be followed by a series of header lines, then the body of the request (the body is typically only present when uploading data via the "POST" or "PUT" methods). In general, various headers may be provided, in different orders, with differing values. However, at least some of the set of headers provided, and the header order, and the header values, are predictable for specific HTTP clients. The following sets of headers, header order, and header values may be provided by a WAP2 browser:

```
GET http://home/ HTTP/1.1
Accept: text/vnd.wap.wml, application/vnd.wap.wmlscriptc,
application/*, application/xhtml+xml, image/vnd.wap.wbmp,
image/gif, image/jpeg, image/png, text/html, text/x-
vCalendar, text/x-vCard, text/css, multipart/*, text/x-co-
desc, text/vn
Accept-Charset: ISO-8859-1, US-ASCII, UTF-8;q=0.800, ISO-
10646-UCS-2;q=0.600
Accept-Language: English, Finnish
x-wap-profile:
http://myclient.profile.com/uaprof/myclient.xml
Cookie2: $Version="1"
Proxy-Connection: Keep-Alive
User-Agent: myclient/2.0 Profile/MIDP-1.0 Configuration/CLDC-
1.0
```

Host: home

- 5 **[0046]** The "Accept" header identifies the MIME types (content formats) supported by the client logic and the client device that is executing the client logic.
- [0047]** The "Accept-Charset" header identifies the character sets that the application supports.
- [0048]** The "Accept-Language" header identifies the languages that the application supports.
- 10 **[0049]** The "x-wap-profile" header is a WAP2-specific header that identifies the location of the User Agent Profile (detailed device capability information) for the client device.
- [0050]** The "Cookie2" header advises the HTTP server that the application understands "new-style" cookies.
- 15 **[0051]** The "Proxy-Connection" header requests that the HTTP server keep the connection open between the application and the server, by communicating periodic Transmission Control Protocol (TCP) "keep-alive" packets.
- [0052]** The "User-Agent" header identifies the HTTP client logic, and is unique to the client logic. It may include information about the vendor, client code source, version, and client device.
- 20 **[0053]** The "Host" header is a request-specific header that identifies where the requested URI is located.
- [0054]** The HTTP client may provide a header including information derived from provision information. The following is one example of such a header.
- x-ATTWS-client:
 vgxuyg239y0fcwecx235136scxdw0988iwuefc0iajs0fcqe0ciq
- 30 **[0055]** The header is named "x-ATTWS-client", but it could have any name different than the names of other headers. The value "vgxuyg239y0fcwecx235136scxdw0988iwuefc0iajs0fcqe0ciq" may be an encoded representation of the User Agent or other header. The

encoding may be based upon provision information, such as the IMSI. The HTTP proxy may interpret the header and compare the result with the User Agent header provided by the HTTP client, to authenticate the HTTP client.

5 **[0056]** The value
 "vgxuyg239y0fcwecx235136scxdw0988iwuefc0iajs0fcqe0ciq" may
 also be a secret, predetermined "signature" value provisioned in the
 client device (communicated from the network to the client device and
 stored therein).

10 **[0057]** Although various examples are presented involving HTTP as
 used by WAP2 clients, similar techniques may be applied to any
 communication protocol. For example, the header set, sequence, and
 content of a WAP Version 1.2.1 Wireless Session Protocol (WSP)
 connect request may be examined to authenticate a WSP client.

15 **[0058]** Figure 8 is a flow chart of an embodiment of a method of
 authenticating client logic according to the total content (header set,
 header order, and header content) of a protocol request. At 802 a
 total is set to zero or some other initial value. At 804 it is determined
 whether there are more header bytes to consider. If not, the method
20 concludes at 812. If there are more header bytes to consider, a check
 is made at 806 to determine whether the byte under consideration is
 an odd number or even numbered byte. If the byte under
 consideration is an odd numbered byte, the byte value is added to the
 total at 808. Otherwise the byte value is subtracted from the total at
25 810. The final total provides a reasonable authentication of the client
 logic according to the entire content of the request.

[0059] Of course, header information may be processed in information
 units other than bytes. For example, header information may be
 processed in words, double words, and so on, depending upon the
30 nature and requirements of the processor and software employed.